FINANCIAL CONDUCT AUTHORITY

How to react to a ransomware attack

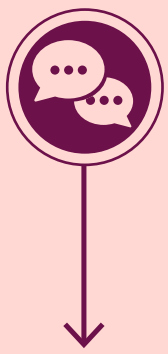
Cyber criminals use ransomware to take control of your data or systems.
They offer to release them if you pay them a ransom.

The National Crime Agency (NCA) strongly advises you not to pay.

Many victims never get their data back and known 'payers' are often targeted again. Read the **National Crime Agency's guidance**.

Tell us

Under our rules you need to tell the FCA as soon as you know of 'material' cyber incidents which affect your firm. This is covered under Principle 11 and relevant provisions in SUP 15.3 of the FCA Handbook.



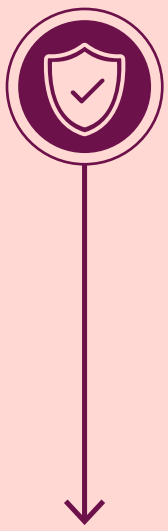
An incident may be material if:

- it could or does result in significant loss of data, or the availability or control of your IT systems
- it affects a significant number of customers and could result in serious harm to them, such as theft of personal data
- it could or does result in someone getting unauthorised access to data and altering it, or
- malicious software is present on your information and IT systems

Find out how to **report an incident to the FCA**.

Protect

To protect yourself, you need to recognise changes in your business risk – and adapt quickly.



1. Do you regularly review the controls that protect the confidentiality, integrity and availability of your business services? Do you review the controls and effectiveness of your third-party suppliers?
2. Do you provide your staff with continuous cyber resilience training, updating it to cover any gaps you've identified? Is this training specifically relevant to staff roles and covers high-risk groups, such as privileged users or users that have access to critical systems?
3. Do you identify and resolve your vulnerabilities quickly? Have you deployed security updates and secure configuration changes to protect your software and devices?
4. Do you use perimeter and end-point malware protection, and make sure they have the most up-to-date signatures and scanning cycles? Do you segment and monitor your network to contain or limit disruption to your business services?

Respond

Ransomware incidents can still occur, so you need to be ready to react.

1. Do you regularly check that your cyber incident response plans – including your third-party support partners' plans – actually work? Have the plans been tested against different scenarios, such as how a ransomware attack might affect your business services?
2. Do your cyber incident response plans prioritise business services?
3. Do your communications response plans include all stakeholders, including customers? Do they cover how you will manage the situation after the event?
4. If an attack happens, do you tell relevant internal and external parties – such as regulators, the NCSC and the NCA - and share relevant data with them?

Recover

How quickly you can restore business services after an incident such as ransomware is critical.

1. Do you maintain adequate secure backups of data and system configuration? Do you carry out testing to ensure you can restore business services if an incident happens?
2. Do you make sure you know which systems and data is required to recover your business services?
3. Do you carry out business-wide 'lessons learned' after an incident? Do you take the appropriate steps to prevent the same types of incidents from happening?

Read the **National Cyber Security Centre's (NCSC's) guidance, including guidance on mitigating malware**.